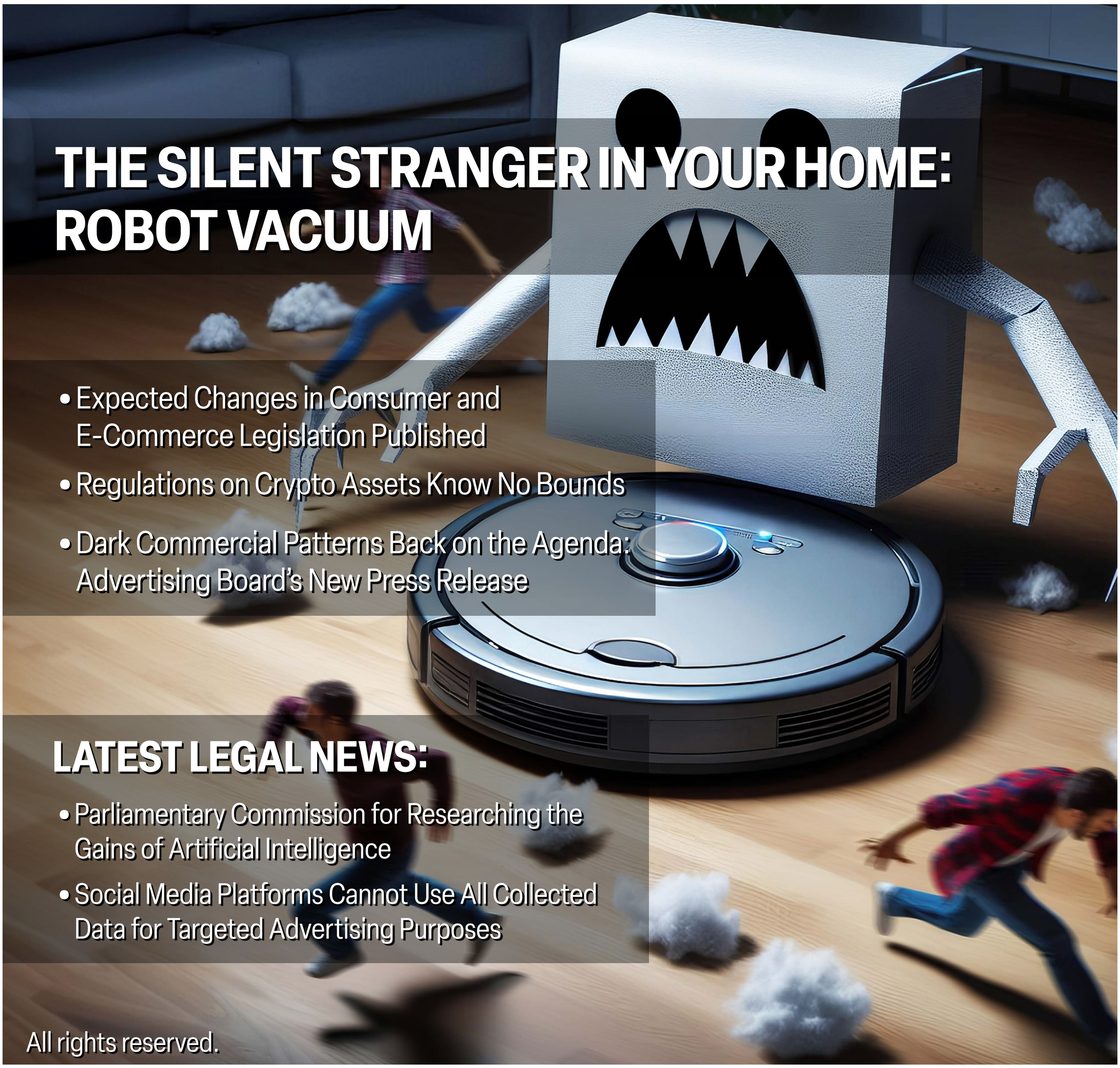
OCTOBER 2024 Gökçe ISSUE: 131

THE FINE PRINT

Answers. Not theories.



THE SILENT STRANGER IN YOUR HOME: ROBOT VACUUM

- Expected Changes in Consumer and E-Commerce Legislation Published
- Regulations on Crypto Assets Know No Bounds
- Dark Commercial Patterns Back on the Agenda: Advertising Board's New Press Release

LATEST LEGAL NEWS:

- Parliamentary Commission for Researching the Gains of Artificial Intelligence
- Social Media Platforms Cannot Use All Collected Data for Targeted Advertising Purposes

The Silent Stranger in Your Home: Robot Vacuum

Robot vacuums from a specific brand have been "hacked" by unknown individuals, despite being located in several different cities across the United States. Owners reported that their vacuums are being physically controlled, emitting obscenities and insults through their onboard speakers, and even chasing their pets. Some videos documenting these incidents have gone viral.

One data subject alleges that he heard sizzling noises coming from his robot vacuum, after which someone connected to the live camera via the vacuum's app. He claims that even after resetting the app's password and restarting the vacuum, it continued to yell insults, with the only solution being to turn it off completely.

People affected by this data breach are nonetheless relieved to be aware of the presence of cyber attackers. These small robots, which have a camera and voice recording functions and can memorize the locations of rooms and items in the house, can lead to significant privacy violations.

The company that manufactures the robot vacuum acknowledges that a cyber-attack occurred but claims that "there is no evidence that it was compromised due to a security vulnerability" in its systems.

The company stated that the data security breach occurred when an individual reused the same username and password across multiple websites, and that this combination was stolen in a separate cyberattack. The company also claimed it had informed the data subjects about significant vulnerabilities in the app in a timely manner. However, the data subjects contended that they were not notified by the company about any such issues.

It is Not Known How Many of the Company's Devices Have Been Hacked in Total

Security researchers believe that this cyber-attack was caused by known security flaws in the system.

The most critical of these security flaws is vulnerability in the Bluetooth connector, which allows full access to the robot vacuum from up to 100 meters away. The company is also known to have experienced other security issues in the past.

A Legal Perspective

As technology becomes increasingly integrated into every aspect of our lives, the number of people concerned about their data being compromised is growing rapidly. This makes data security more critical than ever. Particularly in areas such as Internet of Things (IoT) devices, robots, and automation machines, ensuring data security has become one of the most important measures to counter threats arising from technological advancements.

IoT, one of the most prevalent technologies we encounter in daily life, enables objects equipped with sensors to communicate with each other and with people via the internet. Robot vacuums are a prime example of this. In short, IoT works like this:

- **Data Collection:** Objects are equipped with sensors that collect data from their environment.
- **Data Sharing:** The collected data is transferred to cloud systems. Here, data is securely stored and shared.
- **Data Analytics:** Specialized software in the cloud, analyzes this data and generates meaningful insights.
- **Transmission to the User:** Finally, the analyzed data is made available to users through an application or website and the "output" is realized.

Through this flow, a robot vacuum cleaner can detect objects, record video or audio, obtain data, including data about a person's private life, or can process and analyze data on its own or along with other things. These devices are therefore unarguably well-suited to being targeted by malicious actors.

There are various regulations on this subject across different legal systems. It is widely acknowledged that numerous crimes can arise, including breaches of confidentiality, unauthorized access to information devices, and unauthorized processing of data. In addition, the EU Cybersecurity Act, the NIS2 Directive, and the EU Cyber Resilience Act are critical pieces of legislation. Similarly, in the United States, the IoT Cybersecurity Improvement Act of 2020 plays a crucial role in establishing security standards for these digital devices and the industry as a whole. While there is currently no specific legislation in place in our country, it is possible to note that general protective provisions exist in the Turkish Penal Code and the Personal Data Protection Law.

It is evident that the most crucial issue is the establishment of a system that ensures devices meet specific standards and operate in accordance with security measures before a breach occurs.

As IoT technology continues to permeate every aspect of our lives, the need for special regulations in this area is growing day by day. We are closely monitoring developments both globally and within our country with great interest.

Expected Changes in Consumer and E-Commerce Legislation Published

One of the most dynamic areas in recent regulatory changes in Turkey is undoubtedly consumer and electronic commerce legislation. In this regard, the Draft Law on Amending the Law on Consumer Protection and Certain Other Laws, which proposes changes in these areas, was submitted to the Turkish Parliament on 18 July 2024. You can reach our previous article on the Draft Law in our TFP August issue here.

Draft Law has been accepted for amendments in the e-commerce and consumer legislation and published in the Official Gazette on 30 October 2024. Some of these changes have had effect on the date of publication, while others will come into force after a certain period. The critical points are as follows:

- Consumer credit and housing finance contracts can now be concluded remotely.
- The definition, requirements, and essential features of direct sales systems have been determined and elaborated.
- Advertising Board's authority to impose administrative fines has been increased to 6 million Turkish Liras. Instead of applying a fixed penalty, the Advertising Board can now impose fines based on the assessment of each specific situation.

- Administrative fines imposed by the Advertising Board are now included within the scope of reconciliation.

Changes in E-Commerce Licensing:

As known, intermediary e-commerce service providers are now required to obtain a license under the amended e-commerce legislation. There is a highly complex structure in calculating the license fee.

With the changes, the investment expenses made by intermediary e-commerce service providers and those in economic integrity with them, provided they meet certain conditions and are conducted with an investment incentive certificate, will be deducted from the net transaction volume. These deductions will not exceed 20% of the e-commerce volume calculated by the Ministry.

You can reach the full text of the relevant Law here *(only available on Turkish)*.

Regulations on Crypto Assets Know No Bounds

The Law on Amendments to the Capital Markets Law, which included significant regulations on crypto assets, had been published in the Official Gazette on 2 July 2024 and entered into force with transitional provisions and the Capital Markets Board **(Board)** was authorized to determine the principles regarding the establishment, shareholders, directors and capital of crypto asset service provider companies.

Accordingly, the Board had published its first principal decision on 8 August 2024. The relevant decision included the principles required for platforms where one or more of the crypto asset trading, initial sale or distribution, clearing, settlement, transfer, custody and other transactions that may be determined.

Recently, the Board has published a new principal decision **(Decision)** outlining that there are different practices in the storage of customer cash, customer orders are received via social media, and regulations should be made regarding the listing of crypto assets. It is also emphasized that crypto asset platforms need to be regulated in terms of advertising, announcements and investor protection.

Primary principles in the Decision are as below:

- Accounts opened on behalf of customers should be clearly identified as belonging to platform customers and should not be used for purposes other than the specified purpose.
- Customer orders should only be received through websites, mobile applications or registered phones specified by the platforms. Otherwise, orders received through other methods will be deemed unauthorized activity.
- Transactions such as receiving or delivering cash from customers by hand are prohibited.
- It is regulated that customer orders cannot be received via social media platforms such as WhatsApp and Telegram.
- The cash belonging to customers must be kept in banks, and the accounts opened in the name of the customer cannot be used for any other purpose.
- As emphasized in the Board's previous principal decision, it was underlined again that platforms should only execute customers' cash transfers through authorized banks or institutions.
- Establishing the necessary infrastructure to store the log records of orders with a time stamp and to keep the records in this way as of 8 November 2024; became mandatory.
- It is regulated that NFTs and assets used only in virtual games are outside the scope of the law. It was also stated that the platforms on the list of those operating should put a warning when they list these assets and notify the Board.
- It was regulated that the activities of making regular transactions for commercial purposes on P2P marketplaces on behalf of oneself but on someone else's account should be terminated until 8 November 2024. It was stated that these activities may be considered as unauthorized crypto asset service provision.
- Platforms are required to be objective in their advertisements, announcements and not to use misleading information.
- Promotional campaigns in which any advantage or benefit is provided to the people who bring customers to the platform by any method or to the customers they bring to the platform cannot be organized.
- Promotional campaigns that offer the promise of return (staking) or direct investment in certain crypto assets are prohibited.
- Lending crypto asset transactions, transactions with the purpose of lending and leveraged transactions are prohibited.
- Platforms must provide the necessary technical infrastructure for data transfer to the Central Registry Agency **(CRA)** and perform system integration within the framework of the manner and timetable stipulated by the CRA.
- If crypto assets are not stored in customers' wallets, platforms must ensure the control of wallet keys until 8 November 2024.

This principal Decision could be described as one of the milestones in terms of ensuring order in the crypto asset sector and increasing investor security. Complying with the Decision will not only require platforms to operate within a transparent and legal framework, but it will also be a crucial step in establishing permanence and trust in the sector.

You can reach the full text of the relevant principal decision of the Board here *(only available in Turkish)*.

Dark Commercial Patterns Back on the Agenda: Advertising Board's New Press Release

On 10 September 2024, the Advertising Board **(Board)** convened to evaluate numerous advertisements and commercial practices that are deceptive and misleading to consumers.

The primary focus of the meeting was on **"Dark (Commercial) Patterns"**. Dark Patterns are defined as manipulative and unethical design strategies that lead consumers to make unconscious decisions.

These practices are currently under scrutiny by regulatory authorities. In fact, a protocol was recently signed between the Personal Data Protection Authority and the General Directorate of Consumer Protection and Market Surveillance to address Dark Patterns. The institutions announced their commitment to monitoring these designs to protect consumers and ensure the legitimate use of data. Please see our September TFP on this topic here.

As anticipated, following this collaboration with the Directorate General, the primary focus of this month's Advertising Board meeting was on Dark Patterns. In this context, the Board highlighted several critical points in its decisions and publicly shared its assessments and evaluations regarding Dark Patterns.

- It is mandatory to provide payment method information to access the "free trial" opportunity. However, consumers often seek a trial period because they are unsure about committing to a subscription. This requirement forces consumers to take an action they may not be willing to take, which is unfair;
- Notifications such as *"...person favorited", "... person's basket"* etc. negatively influence consumers' will to make a decision or choice;
- Making the colors of the area or button that the consumer is directed to more eye-catching and prominent is also a form of manipulation;
- Although the updated subscription agreement explicitly includes the word "accept," the consumer is not given the opportunity to "reject" the offer. The "Continue" option is more prominently designed than the "X" sign, exemplifying the use of Dark Patterns.

The Board also evaluated the recent emphasis on "popularity" in advertisements and promotions. It concluded that if phrases such as "most popular" and "most preferred" are highlighted in relation to subscription packages, the specific metrics behind these claims (such as the number of purchases, clicks, or additions to the basket) should be clearly and explicitly stated.

In line with the above-mentioned practices, the Board concluded that the deceptive and misleading company practices are Dark Patterns and imposed administrative sanctions.

You can reach the related press release here *(only available in Turkish)*.

Parliamentary Commission for Researching the Gains of Artificial Intelligence

The "Decision on the Establishment of a Parliamentary Research Commission for the Purpose of Determining the Steps to be Taken for the Gains of Artificial Intelligence, Establishing the Legal Infrastructure in this Field and Determining the Measures to Prevent the Risks of the Use of Artificial Intelligence" is published on the Official Gazette dated 5 October 2024.

It is seen by the decision that a parliamentary research commission will be constituted to determine the steps that can be taken regarding the development of artificial intelligence nowadays. The commission, whose working period is set as 3 months, consists of 22 members. The commission aims to examine the social, economic and ethical dimensions of artificial intelligence in depth.

These developments will create a significant road map in terms of managing both the opportunities and benefits created by artificial intelligence and its risks. In these days when artificial intelligence increases its effectiveness globally and its impact on our life day by day. The activities of the research commission to be assembled in the coming days are a matter of curiosity.

You can access the relevant the Grand National Assembly of Turkey decision here *(only available in Turkish)*.

Recent Judgement of the Court of Justice of the European Union: Social Media Platforms Cannot Use All Collected Data for Targeted Advertising Purposes

Some recent decisions of the Court of Justice of the European Union **(CJEU)** were published in a press release on 4 October 2024. The judgements are again significant in terms of personal data. Among the published judgements, the most striking one is C-446/21, which determines the CJEU's stance against the violating actions of Meta platforms regarding personal data.

The judgment emphasizes that a social media network like Facebook cannot use all the personal data it collects for targeted advertising purposes without time restrictions or distinctions based on data type. To summarize the case, it all started when Maximilian Schrems, an activist, made a statement about his sexual orientation on a public panel. Schrems did not share this data on Facebook; rather, he disclosed it verbally during a panel where he participated as a speaker. Subsequently, he began regularly receiving targeted advertisements for homosexuals and invitations to related events on Facebook, via one of Meta's platforms. This indicates that Facebook, as part of Meta, also collects and processes non-Facebook data about its users.

The central argument in this case is whether Schrems has consented to the processing of this data under the GDPR, given that he explicitly disclosed sensitive personal information by publicly revealing his sexual orientation during a panel discussion. Although he verbally shared this information in a public setting, it was not posted on any social media platform, and no consent was provided for the processing of such data by any social media network.

In its decision, the CJEU examines the relevant GDPR provisions by addressing two key questions: the processing of publicly disclosed personal data without consent, and its use for targeted advertising purposes:

- **Should Article 5(1)(c) GDPR be interpreted as meaning that all personal data held by a platform can be used for targeted advertising without time or data type restrictions, as in the main proceedings?**

GDPR art. 5/1-c regulates the data minimization principle. As per the relevant article of GDPR, personal data should be limited to sufficient, relevant and necessary for the processing reasons. The CJEU stated that the principle of data minimization excludes all personal data obtained from the data subject or third parties, whether collected on or off the social media platform, for targeted advertising purposes. It also clarified that this restriction is not subject to time limitations or differentiation by data type regarding the collection, analysis, and processing of the data.

- **Should Article 5(1)(b) of the GDPR, taken in conjunction with Article 9(2)(e), be interpreted as meaning that a statement made by an individual about their sexual orientation during a panel discussion is consent to the processing of other data relating to sexual orientation for the purpose of collecting/analyzing data for personalized advertising purposes?**

Art. 9 GDPR regulates the processing of special categories of personal data. Article 9(2) (e) of the GDPR, which is the provision that was referred to by the Court, sets forth that the data processed must relate to matters that the data subject has expressly made public. Ultimately, the CJEU answered this question by stating that "*...a statement made by the data subject about his or her sexual orientation during a public panel discussion may constitute an act by which the data subject has expressly made such data public within the meaning of Article 9(2)(e) GDPR. However, this alone does not authorize the processing of this data for the purpose of aggregating and analyzing the data for the purpose of personalized advertising.*"" Accordingly, it was concluded that public disclosures do not grant the social media platform the right to engage in targeted advertising based on the content of the disclosure.

Additionally, according to the decision, Meta can only utilize a portion of its data pool, even if users consent to targeted advertising.

This decision is significant as it prohibits the social media platform from spontaneously processing personal data that the data subject has publicly disclosed, as well as any other data that may be linked to this information.

You can reach the relevant press release from here *(available in EU languages)* and the mentioned CJEU decision from here *(available in EU languages)*.

Editors

Görkem Gökçe
gorkem.gokce@gokce.av.tr

Dr. Mehmet Bedii Kaya
bedii.kaya@gokce.av.tr

Elif Aksöz
elif.aksoz@gokce.av.tr

Yağmur Yollu
yagmur.yollu@gokce.av.tr

About us

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at
info@gokce.av.tr
0 212 352 88 33